

January 11, 1994

BOOKLET COPY ORIGINAL

RECEIVED

JAN 25 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

One

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Tough T. Brest
LEDERLE LABORATORIES
401 N. MIDDLETOWN RD
PEARL RIVER NY 10965



The University of
Puget Sound

DO NOT FILE COPY ORIGINAL

January 14th, 1994

Mr William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Reference: CC Docket 93-292

RECEIVED
JAN 25 1994
FCC - MAIL ROOM

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning toll fraud. As a telecommunications profession, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the interstate carriers (IXC) and the customer premise equipment (CPE) vendors, I can still experience toll fraud. It is impossible to secure my telephone system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided by IXCs, CPEs, and Local Exchange Companies (LECs), the law should reflect that. It is preposterous to think that IXCs, LECs, and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While programs offered by IXCs have broken new ground in relation to preventing toll fraud, they still don't do much. Some of these services are too expensive for small companies and the educational information is superficial. Monitoring by the IXCs should be part of the basic interexchange service offerings, as all companies, large or small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any case of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

Orig.

Ltr To: William F. Canton
Re: CC Docket 93-292
Date: January 14th, 1994
Page 2

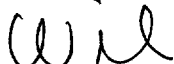
JAN 25 1994

FCC - MAIL ROOM

I applaud the provisions outlined in the docket on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with the features of the CPE, and the IXCs and LECs to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have meet the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally. Remember -- shared liability addresses the symptom of the problem of toll fraud and not the cause. Adequate law enforcement methods should be defined and implemented to catch and prosecute hackers who perpetrate toll frauds.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make positive impact on this terrible problem.

Sincerely yours,



~~WILFREDO R. RODRIGUEZ~~

Mail and Telephone Systems Coordinator

cc John Hickey

January 11, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

JAN 25 1994

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Orig.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in black ink, appearing to read "John Redman". The signature is fluid and cursive, with the first name "John" and last name "Redman" clearly distinguishable.

January 11, 1994

FORGET FILE COPY ORIGINAL

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

JAN 25 1994

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Quigley

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Joanne DeLuca
American Life Insurance

January 11, 1994

DOCKET FILE COPY ORIGINAL

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

JAN 25 1994

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Aug

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

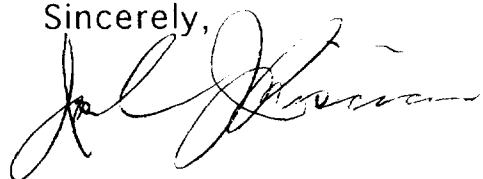
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC(s) and LEC(s) to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in black ink, appearing to read "J. L. Harrison". The signature is fluid and cursive, with a long horizontal stroke at the end.



1500 Cader Lane • P.O. Box 6002, Petaluma, CA 94953-6002 • (707) 763-9911 • FAX (707) 765-1378

DO NOT WRITE COPY ORIGINAL

January 10, 1994

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

1-10-94

JAN 25 1994

FCC - MAIL ROOM

RE: CC Docket 93-292

Dear Mr Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXC's and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs, and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing to fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs

No. of Copies rec'd
List ABCDE

should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

Evelyn Hill/Telecommunications Coordinator

Evelyn Hill



Hercules Incorporated
Hercules Plaza
Wilmington, DE 19894
(302) 594-5000
Telex: 83-5479

January 17, 1994

RECEIVED

JAN 25 1994

FCC - MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint GuardTM, MCI DetectTM, and AT&T NetprotectTM) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd Aug.
List ABCDE

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll fraud is a financially devastating problem that effects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,



P. A. Derosier
Consulting Telecommunications Engineer
IMCO Services

Pad/nv

No. of Copies rec'd
List ABCDE



January 11, 1994

DOCKET FILE COPY ORIGINAL

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

JAN 25 1994

FCC - MAIL ROOM

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXCs, LECs and CPE vendors. The legal obligations of the IXCs, LECs and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXCs (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXCs must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LECs must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Quigley

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Newton Memorial Hospital
Newton N.J. 07860.

DOCKET FILE COPY ORIGINAL

RECEIVED

January 11, 1994

JAN 23 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

Re: CC Docket no. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my company's telecommunication systems and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features but by the information, equipment and services provided by IXC's, LEC's and CPE vendors. The legal obligations of the IXC's, LEC's and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

No. of Copies rec'd
List ABCDE

Orig.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security related hardware and software in the price of their systems.

The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the;

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s) and IXC(s) involved.

Toll Fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors and carriers. I am sure, that if we all work together we can and will make a positive impact on this problem.

Sincerely,

Collin R. McBride
United Missouri Bank



January 11, 1994

C.R. Laurence Co., Inc.
Glaziers', Industrial, Construction
and Automotive Supplies

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, D.C. 20554

FCC - MAIL ROOM
JAN 25 1994

RE: CC Docket 93-292

Dear Mr. Canton:

It was with great interest I read the recent FCC Notice of Proposed Rulemaking concerning Toll Fraud. As a telecommunications professional who is responsible for my company's communications systems, I am encouraged by the proposed rulemaking because even though I have taken each and every protective step recommended by the IXCs and CPE vendors to secure my systems, I can still experience toll fraud. It is impossible to secure my system 100% from fraud.

It is with some very tangible knowledge that we are writing this letter of support as we were hit for \$35,000 in Toll Fraud over two years ago. We have proven that we were hit as a direct result of our vendors lack of timeliness in informing us of a suspected problem.

PBX owners should not be responsible for 100% of the toll fraud if we don't control 100% of our destiny. Since our destiny is not only controlled by our PBX security precautions, but also by the information, services and equipment provided IXCs, LECs and CPEs, the law should reflect that. It is preposterous to think that the IXCs, LECs and CPEs who all have a very important part in this issue, have absolutely no legal obligations to warn customers and therefore, no real incentive to stop fraud.

CPEs should be required to provide warnings about the risks of toll fraud with their equipment and provide recommended counter methods. It is critical that CPEs ship equipment without default passwords which are well known within the hacker community. Passwords should be created during the installation of the equipment with the customers full knowledge. CPEs should be required to include security-related hardware and software in the price of their systems. When you buy a car, the lock and key are provided in the design and price of the car. Not an adjunct that you have to purchase later.

While the programs offered by IXCs, such as MCI Detect, AT&T NetProtect and Sprint Guard have broken new ground in relation to preventing toll fraud, they still don't do enough. Some of these services are too expensive for smaller companies and the educational information is superficial. Monitoring by the IXCs should be a part of the basic interexchange service offerings, as all companies, large and small, are vulnerable to toll fraud. If the IXCs were monitoring all traffic, there wouldn't be any cases of toll fraud for periods longer than a day.

No. of Copies rec'd
List ABCDE

047

As hackers begin new methods of breaking in to systems by using local lines instead of 800 numbers, the LECs should be required to offer monitoring services similar to the IXC's.

I applaud the provisions outlined in the NPRM on shared liability. They are fair and equitable. Shared liability will require clear definitions of the specific responsibilities of the CPPE owner to secure their equipment, the manufacturer to adequately warn the customer of the toll fraud risks associated with features of the CPE, and the IXC's and LEC's to offer detection and prevention programs and educational services. If toll fraud occurs and one of the parties should fail to meet these responsibilities and prove to be negligent, then they should bear the cost of the fraud. I do not believe any damages should be awarded to the aggrieved parties. Should all parties have met the aforementioned responsibilities, and toll fraud occurs, then liability should be shared equally.

However, shared liability only addresses the symptom of the problem of toll fraud and not the cause.

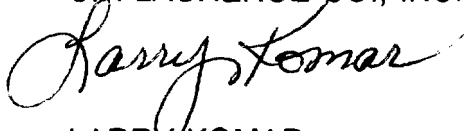
The root of this insidious crime of toll fraud is the hacker community. As the information highway widens, so do the endless opportunities for hackers to compromise our communication systems. I do not believe it when the hackers state they only "hack" to gain knowledge. If this were the case, there wouldn't be a toll fraud problem. While it is the hacker who breaks in to the systems and sells the information, it is the call sell operations that truly profit from it.

Until we come up with an adequate method of law enforcement to catch and prosecute these criminals, toll fraud will continue to grow beyond the \$5 billion problem it is today. We must develop legislation that clearly defines and penalizes this criminal activity and gives law enforcement the tools it needs to track and prosecute the perpetrators of toll fraud.

Toll fraud is an illegal, fraudulent theft of service. I am encouraged that if we all work together we can make a positive impact on this terrible problem.

Sincerely,

C.R. LAURENCE CO., INC.

A handwritten signature in cursive script that reads "Larry Komar".

LARRY KOMAR

Telecommunications Manager



Communications Fraud Control Association

1990 M Street, N.W. Suite 508 • Washington, DC 20036 • Phone (202) 296-3225 • Fax (202) 296-3268

DOCKET FILE COPY ORIGINAL

JAN 25 1994

President

Thomas Schutz
MCI
(312) 938-4663

Vice President

Willeen Duncan
AT&T
(404) 552-2110

Treasurer

Marty Locker
LDDS Metromedia
Communications
(201) 804-7016

Secretary

Dana Bruce Berry
LINKUSA
(319) 363-7570

**Immediate
Past President**

Clo Fleming
Sprint
(913) 624-4721

Directors

Barry Berman
US Tele-Comm
(516) 829-2000

Judy Betts
LCI Intl
(614) 798-6379

Linda Giles
One Call
(317) 580-7127

Susan Gregersen
LDDS Metromedia
Communications
(601) 364-7063

Jerry H. Griffey
ONCOR
(214) 902-6466

Joseph Mansfield
EDS
(313) 262-7470

James Waltman
US WEST
(303) 896-3021

Executive Director

Frances Feld, CAE

January 14, 1994

Office of the Secretary
Federal Communications Commission
Washington, DC 20554

re: CC Docket 93-292

Gentlemen:

Enclosed you will find our comments to the above captioned.

Each Commissioner is to receive a personal copy, therefore we are enclosing an original plus nine copies.

Sincerely,

Frances Feld, CAE
Executive Director

enc: as stated

No. of Copies rec'd
List ABCDE

049



Communications Fraud Control Association

1990 M Street, N.W. Suite 508 • Washington, DC 20036 • Phone (202) 296-3225 • Fax (202) 296-3268

JAN 25 1994

President

Thomas Schutz
MCI
(312) 938-4663

Vice President

Willeen Duncan
AT&T
(404) 552-2110

Treasurer

Marty Locker
LDDS Metromedia
Communications
(201) 804-7016

Secretary

Dana Bruce Berry
LINKUSA
(319) 363-7570

Immediate

Past President

Clo Fleming
Sprint
(913) 624-4721

Directors

Barry Berman
US Tele-Comm
(516) 829-2000

Judy Betts
LCI Intl
(614) 798-6379

Linda Giles
One Call
(317) 580-7127

Susan Gregersen
LDDS Metromedia
Communications
(601) 364-7063

Jerry H. Griffey
ONCOR
(214) 902-6466

Joseph Mansfield
EDS
(313) 262-7470

James Waltman
US WEST
(303) 896-3021

Executive Director
Frances Feld, CAE

Before the Federal Communications Commission Washington, D.C. 20554

In the Matter of)
Policies and Rules) CC Docket No. 93-292
concerning Toll Fraud)

Comments From the Communications Fraud Control Association

The Communications Fraud Control Association (CFCA) was founded in 1985, with the sole purpose of combatting toll fraud in the telecommunications industry. The membership is made up of local and inter exchange carriers, end users, vendors and law enforcement. CFCA is proud of its reputation as an industry leader in this fight.

CFCA has reviewed the proposed ruling and is pleased that the FCC is focusing on an issue that is of great concern to its membership. We believe that the prevention through education should be stressed as the primary solution.

In the area of CPE fraud, the technical capabilities to prevent fraud vary with the many types of customer provided equipment. And, the customers are the most familiar with their legitimate calling patterns. The customers must be educated about the various fraud schemes, the indicators that fraud may be present and the actions that may be taken once fraud occurs. The level of knowledge varies.

Many carriers have aggressive customer education programs while some also offer monitoring services. Fraud is volatile and rapidly moves around the industry to the weakest link. When one weakness is corrected, the fraud community quickly finds another. The industry has yet to find a solution that will stop the problem. Minimizing the problem requires that everyone be knowledgeable and aware at all times. Companies and individuals working together to identify the individuals and the weaknesses in the systems/processes.

In summary, CFCA believes that proactive, aggressive education programs is the most effective tool against combatting this type of fraud, along with stringent enforcement of the laws accompanied by maximum penalties for abusers.

Respectfully submitted,
CFCA Board of Directors

By: *Frances Feld*

Frances Feld, CAE, Executive Director January 14, 1994